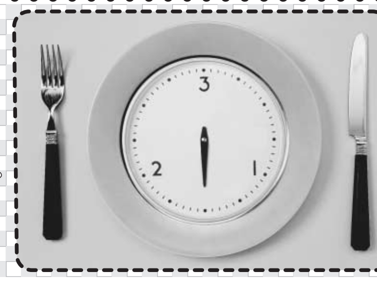
Cベース設計 3分間クッキング



第10回　スタティック検証

鮫島正裕

このところしごとが詰まって，徹夜をするようになってしまった．徹夜をしていると，なぜか魚肉ソーセージが食べたくなる．近所の特売で買ってきて，そのまま食べたり，キャベツと卵でいためたりしている．

魚肉ソーセージを食べながら，はいだ包みを読んでいると，「HACCP承認」と書いてあることに気がついた．調べてみると，HACCPは食品の品質の管理方法で，Hazard Analysis and Critical Control Pointの略．日本語訳は「危害分析・重要管理点」だそうで，なんとNASA（米国航空宇宙局）で生まれた手法らしい．

宇宙に行っているときに食中毒になっても，今のところすぐには病院に行けないので，宇宙食にはそれなりの品質が求められる．最終工程の抜き取り試験といった管理手法では，抜き取らなかった食品に「あたり」が混ざっていないことを保証できない．そのためHACCPでは，製造工程のどの部分にどの程度の病原菌や科学的な危害の原因があるか，病原菌の増殖速度や滅菌工程における減少数，その食品がどのような状況で食べられるかを検討する．また，作業の手順とそのチェック方法を決めて，さらに工程の維持管理方法も定めて製造する．HACCPによる工程管理で作られたものは，「あたらない」と保証される．深夜，魚肉ソーセージを食べながら，なんとなく，スタティックな（静的な）気分になったりしている．

＊　　＊　　＊

C言語の開発環境でスタティックに検証するものとしては，コンパイラのオプションによるワーニングやフォーマル検証，その中間に位置するLint系のツールなどがある．

リスト1は，CygwinやLinux系の環境に含まれるSplintのAnnotationを追加したANSI Cの例である．このソースを`gcc -Wall`でコンパイルしてもエラーやワーニングは出力されないが，31～33行目に問題があり，おかしな動作をする．2～21行目は文字列をコピーする関数で，`/*@　@*/`で囲まれたコメントがSplintのAnnotation．ポインタ変数の入出力の規定，およびデータの変更範囲の規定や保証の設定を行っている．これを`splint +bounds [list.c]`で実行すると，28，31，32，33行目でエラーが報告される．28行目は`p2`が入力として関数に与えられているが，初期化が27行目の1要素だけのため，「初期化が完全ではない」というエラーとなる．

リスト1　SplintのAnnotation

```
 1  #include<stdio.h>
 2  static void
 3  test(
 4        /*@unique@*/
 5        /*@returned@*/
 6        /*@out@*/  char *data_o,
 7        /*@in@*/   char *data_i,
 8        int size)
 9  /*@modifies *data_o@*/
10  /*@requires maxSet(data_o) >= (size-1)
11           /¥ maxRead(data_i) >= (size-1)
12           /¥ size >= 1                @*/
13  /*@ensures maxRead(data_i) >= maxRead(data_o)
14           /¥ maxRead(data_i) <= size; @*/
15  {
16    int i = size-1;
17    do{
18        data_o[i] = data_i[i];
19        i--;
20    } while(i>=0);
21  }
22
23  int main()
24  {
25    char p2[8], p3[8];
26
27    p2[6] = '¥0';
28    test(p3, p2 ,6);
29    test(p2,"123456",6);
30    test(p3, p2 ,6);
31    test(p3,"123456",9);
32    p2[11]='A';
33    test(p3,"0123456789",10);
34    printf("%s¥n",p2);
35    return 0;
36  }
```

28行目と同じ30行目では，29行目の呼び出しで`p2`が保証されているためエラーとはならない．31～33行目は配列の範囲外アクセスとして報告される．

＊　　＊　　＊

Lint系のツールはあれこれ細かいことにうるさいので，ついつい無視してしまうことがあるが，製造（コーディング）工程における管理が重要ですよと，魚肉ソーセージに教わりました．

＜筆者プロフィール＞
鮫島正裕（さめしま・まさひろ）．高速ディジタル回路のコンサルティングやEDAツール関係のしごとに従事．